

Canonical representatives for residue classes of a polynomial ideal and orthogonality

Edgar Delgado-Eckert^{*†‡}

Abstract

The aim of this paper is to unveil an unexpected relationship between the normal form of a polynomial with respect to a polynomial ideal and the more geometric concept of orthogonality. We present a new way to calculate the normal form of a polynomial with respect to a polynomial ideal I in the ring of multivariate polynomials over a field K , provided the field K is finite and the ideal I is a vanishing ideal. In order to use the concept of orthogonality, we introduce a symmetric bilinear form on a vector space over a finite field.

Keywords: Polynomial algebras, polynomial ideals, Gröbner bases, inner products, normal form

Mathematics Subject Classification: 13P10; 15A63

1 Introduction

A well known result of B. Buchberger is the existence of the normal form of a polynomial with respect to a polynomial ideal I in the ring of multivariate polynomials over a field K . This result follows from the existence of so called Gröbner bases for polynomial ideals. For a given fixed term ordering, this normal form is unique (Lauer, 1976), (Buchberger, 1976), (Buchberger, 1970). In this paper we present a new way to calculate this normal form, provided the field K is finite and the ideal I is a vanishing ideal, i.e. I is equal to the set of polynomials which vanish in a given set of points X . Our method doesn't pursue establishing a new, especially efficient, algorithm for the computation of such a normal form. Rather, the aim of this paper is to unveil an interesting way to look at this issue based on the concept of orthogonality.

For orthogonality to apply, we introduce a symmetric bilinear form on a vector space (see, for instance, (Scharlau, 1969)). A symmetric bilinear form can be seen as a generalized inner product. Some authors have explored vector spaces endowed with generalized forms of inner products. For example, we refer to the following papers: (Lumer, 1961), (Barbieri & Facchinetti, 1973), (Degani Cattelani & Fiocchi, 1974), (Degani Cattelani & Fiocchi, 1975), (Mininni & Muni, 1979), (Kasahara, 1980), (Vasanth & Johnson, 2003).

^{*}Centre for Mathematical Sciences, Munich University of Technology, Boltzmannstr.3, 85747 Garching, Germany.

[†]Pathology Department, Tufts University, 150 Harrison Av., Boston, MA 02111, USA (correspondence address).

[‡]The author acknowledges support by a Public Health Service grant (RO1 AI062989) to David Thorley-Lawson at Tufts University, Boston, MA.

Having defined a symmetric bilinear form, we are able to introduce the notion of orthogonality and orthonormality. Then we consider the orthogonal solution of a solvable inhomogeneous under-determined linear operator equation. If one thinks of an inhomogeneous under-determined system of linear equations in an Euclidean space, the orthogonal solution is simply the solution that is perpendicular to the affine subspace associated with the system. After going through existence and uniqueness considerations, we come to the main statement of this paper, namely, that the above mentioned normal form can be obtained as the orthogonal solution of a system of linear equations. That system of equations arises as a linear formulation of the multivariate polynomial interpolation problem.

Based on our literature research, we believe that the study of polynomial algebras in the framework of symmetric bilinear spaces (vector spaces endowed with a symmetric bilinear form) represents a novel approach. Suitable extensions of our method to more general fields (i.e. infinite fields) could open new possibilities for studying problems in the areas of polynomial algebra, computational algebra and algebraic geometry using functional analytic or linear algebraic techniques.

The concept of orthogonal solution is not limited by monomial orders, as it is the case for Gröbner bases calculations. In this sense, our method reveals a wider class of normal forms (with respect to vanishing ideals) in which the normal forms à la Buchberger appear as special cases.

Another application that we will describe in detail elsewhere is the problem of choosing a particular interpolant among all possible solutions of a highly under-determined multivariate interpolation problem. This is related to the study of the performance of so called "reverse engineering" algorithms such as the one presented in (Laubenbacher & Stigler, 2004).

The organization of this article is the following:

Section 2 is devoted to the general definition of *symmetric bilinear spaces* and *orthogonal solutions* of an inhomogeneous linear operator equation. Subsection 2.1 covers basic definitions and properties of symmetric bilinear spaces, in particular, the concepts of *orthogonality* and *orthonormality* are introduced. Subsection 2.2 introduces the notion of orthogonal solution of a solvable under-determined linear operator equation. Existence and uniqueness of orthogonal solutions are proved and some issues regarding the existence of orthonormal bases are discussed.

Section 3 deals with the vector space of functions $F : K^n \rightarrow K$, where K is a finite field and $n \in \mathbb{N}$. In subsection 3.1 we paraphrase the known result that all the functions in that space are polynomial functions. Subsection 3.2 introduces a linear operator called *evaluation epimorphism* and formulates the multivariate polynomial interpolation problem in a linear algebraic fashion.

Section 4 covers the more technical aspect of constructing special symmetric bilinear forms. Using that type of symmetric bilinear form will allow us to prove the main result of this article in section 5.

Section 5 is devoted to the statement and proof of our main result. Namely, that the canonical normal form of an arbitrary polynomial f with respect to a vanishing ideal $I(X)$ in the ring of multivariate polynomials over a finite field K can be calculated as the orthogonal solution of a linear operator equation involving the evaluation epimorphism.

For standard terminology, notation and well known results in computational algebraic geometry and commutative algebra we refer to (Cox *et al.* , 1997) and (Becker & Weispfenning, 1993).

2 Symmetric bilinear vector spaces and orthogonal solutions of inhomogeneous systems of linear equations

2.1 Basic definitions

In this subsection we will introduce the concept of a symmetric bilinear form in a vector space. With this concept it will be possible to define symmetric bilinear vector spaces and orthonormality. Furthermore, some basic properties are briefly reviewed (cf. (Scharlau, 1969))

Definition 1 Let V be a vector space over a field K . A symmetric and bilinear mapping

$$\langle \cdot, \cdot \rangle : V \times V \rightarrow K$$

is called symmetric bilinear form on V .

Definition 2 (Notational Definition) Let be $n, m \in \mathbb{N}$ natural numbers and K a field. The set of all $m \times n$ matrices (m rows and n columns) with entries in K is denoted by $M(m \times n; K)$.

Remark 3 Let V be a finite dimensional vector space over a field K . After fixing a basis (u_1, \dots, u_d) of V , it is a well known result, that there is a one-to-one correspondence between the set of all symmetric bilinear forms on V and the set of all $d \times d$ symmetric matrices with entries in K seen as representing matrices with respect to the basis (u_1, \dots, u_d) .

Definition 4 A vector space V over a field K endowed with a symmetric bilinear form

$$\langle \cdot, \cdot \rangle : V \times V \rightarrow K$$

is called a symmetric bilinear space.

Example 5 Every (real) Euclidean space is due to the positive definiteness of its inner product a symmetric bilinear space.

Given a symmetric bilinear space V over a field K , *orthogonality* and *orthonormality* of two vectors $v, w \in V$ as well as the concept of *orthonormal basis* are defined exactly as in the Euclidean case. Similarly, the *orthogonal complement* $W^\perp := \{v \in V \mid v \perp w \ \forall w \in W\}$ of a subspace $W \subseteq V$ is a subspace of V . Furthermore, if (w_1, \dots, w_d) is an orthonormal basis of V , then for every vector $v \in V$ holds

$$v = \sum_{k=1}^d \langle v, w_k \rangle w_k$$

where the field elements $\langle v, w_i \rangle \in K$, $i = 1, \dots, d$ are the well known *Fourier coefficients*. Contrary to the case of Euclidean or unitary vector spaces, in symmetric bilinear spaces orthonormal bases don't always exist.

Example 6 Let $d \in \mathbb{N}$ be a natural number and V a d -dimensional vector space over a field K . Furthermore let (u_1, \dots, u_d) be a basis of V . Then one can construct a symmetric bilinear form on V by setting

$$\langle u_i, u_j \rangle := \delta_{ij} \ \forall i, j \in \{1, \dots, d\}$$

(see also Remark 3.) Here the basis (u_1, \dots, u_d) is obviously orthonormal.

2.2 Orthogonal solutions of inhomogeneous linear operator equations

Definition 7 Let $d \in \mathbb{N}$ be a natural number and V a d -dimensional symmetric bilinear space over a field K . Furthermore, let W be an arbitrary vector space over the field K , $T : V \rightarrow W$ a non-injective linear operator and $w \in W$ a vector with the property

$$w \in T(V)$$

Now let $m := \text{nullity}(T) \in \mathbb{N}$ be the dimension of the kernel of T . A solution $v^* \in V$ of the equation

$$Tv = w$$

is called *orthogonal solution*, if for an arbitrary basis (u_1, \dots, u_m) of $\ker(T)$ the following orthogonality conditions hold

$$\langle u_i, v^* \rangle = 0 \quad \forall i \in \{1, \dots, m\}$$

Remark 8 Let (u_1, \dots, u_m) be a basis of $\ker(T)$. Then each arbitrary vector $u \in \ker(T)$ can be written in the form

$$u = \sum_{i=1}^m \lambda_i u_i$$

with suitable field elements $\lambda_i \in K$. If the orthogonality conditions

$$\langle u_i, v^* \rangle = 0 \quad \forall i \in \{1, \dots, m\}$$

hold for the basis (u_1, \dots, u_m) , then we have

$$\langle u, v^* \rangle = \left\langle \sum_{i=1}^m \lambda_i u_i, v^* \right\rangle = \sum_{i=1}^m \lambda_i \langle u_i, v^* \rangle = 0$$

and that means

$$v^* \in \ker(T)^\perp$$

In particular, for any other different basis (w_1, \dots, w_m) of $\ker(T)$ it holds

$$\langle w_j, v^* \rangle = 0 \quad \forall j \in \{1, \dots, m\}$$

Theorem 9 Let $d \in \mathbb{N}$ be a natural number and V a d -dimensional symmetric bilinear space over a field K . Furthermore, let W be an arbitrary vector space over the field K , $T : V \rightarrow W$ a non-injective linear operator and $w \in W$ a vector with the property

$$w \in T(V)$$

If $\ker(T)$ has an orthonormal basis, then the equation

$$Tv = w$$

has always a unique orthogonal solution $v^* \in V$.

Proof. Let $m := \text{nullity}(T) = \dim(\ker(T)) \in \mathbb{N}$ be the dimension of the null space of T and (u_1, \dots, u_m) an orthonormal basis of $\ker(T)$. Since $w \in T(V)$, there must exist a solution $\hat{\xi} \in V$ of $Tv = w$. For any other solution $\xi \in V$ we have

$$T(\xi - \hat{\xi}) = T(\xi) - T(\hat{\xi}) = 0$$

and therefore

$$\xi - \hat{\xi} \in \ker(T)$$

That means that all solutions $\xi \in V$ of $Tv = w$ can be written in the form

$$\xi = \hat{\xi} + \sum_{i=1}^m \lambda_i u_i$$

with the $\lambda_i \in K$, $i = 1, \dots, m$ running over all K . In particular, we can construct a very specific solution by choosing the parameters $\lambda_i \in K$, $i = 1, \dots, m$ in the following manner

$$\lambda_i := -\langle u_i, \hat{\xi} \rangle, \quad i = 1, \dots, m$$

For this solution

$$v^* := \hat{\xi} + \sum_{i=1}^m -\langle u_i, \hat{\xi} \rangle u_i$$

and for every $j \in \{1, \dots, m\}$ it holds

$$\begin{aligned} \langle u_j, v^* \rangle &= \left\langle u_j, \hat{\xi} + \sum_{i=1}^m -\langle u_i, \hat{\xi} \rangle u_i \right\rangle = \langle u_j, \hat{\xi} \rangle + \sum_{i=1}^m -\langle u_i, \hat{\xi} \rangle \langle u_j, u_i \rangle \\ &= \langle u_j, \hat{\xi} \rangle + \sum_{i=1}^m -\langle u_i, \hat{\xi} \rangle \delta_{ji} = \langle u_j, \hat{\xi} \rangle - \langle u_j, \hat{\xi} \rangle = 0 \end{aligned}$$

This shows the existence of an orthogonal solution of $Tv = w$. Now let $\tilde{v} \in V$ be another orthogonal solution of $Tv = w$. Again, since

$$T(v^* - \tilde{v}) = T(v^*) - T(\tilde{v}) = 0$$

we can write

$$v^* = \tilde{v} + \sum_{i=1}^m \alpha_i u_i$$

with suitable $\alpha_i \in K$. From the orthogonality conditions for v^* and \tilde{v} we have $\forall j \in \{1, \dots, m\}$

$$\begin{aligned} 0 &= \langle u_j, v^* \rangle = \left\langle u_j, \tilde{v} + \sum_{i=1}^m \alpha_i u_i \right\rangle = \langle u_j, \tilde{v} \rangle + \left\langle u_j, \sum_{i=1}^m \alpha_i u_i \right\rangle \\ &= \sum_{i=1}^m \alpha_i \langle u_j, u_i \rangle = \sum_{i=1}^m \alpha_i \delta_{ji} = \alpha_j \end{aligned}$$

and that means $v^* = \tilde{v}$. ■

Remark 10 *The existence of an orthonormal basis of $\ker(T)$ is crucial for the proof of this theorem. It is important to notice that in a symmetric bilinear space over a general field K , the Gram-Schmidt orthonormalization only works if the norm*

$$\|v\| := \sqrt{\langle v, v \rangle}$$

of the vectors used in the Gram-Schmidt process exists in the field K and is not equal to the zero element. In general terms, the existence of square roots would be assured in a field K which satisfies

$$\forall x \in K \exists y \in K \text{ such that } y^2 = x \quad (1)$$

Now, if K is finite, then (1) holds if and only if $\text{Char}(K) = 2$.

After fixing a basis (u_1, \dots, u_d) for the vector space V , the question whether $\langle v, v \rangle = 0$ for $v \neq 0$ is equivalent to the nontrivial solvability in K^d of the following quadratic form

$$\vec{x}^t A \vec{x} = 0 \quad (2)$$

where A is the representing matrix of $\langle \cdot, \cdot \rangle$ with respect to the basis (u_1, \dots, u_d) (see Remark 3). In chapter 3, §2 of (Lidl & Niederreiter, 1997) explicit formulas for the exact number of solutions in K^n of equations of the type (2), where A is a $n \times n$ symmetric matrix with entries in a finite field K , can be found.

Corollary 11 *Let K , d , V , W and T be as in the theorem above. If $\ker(T)$ has an orthonormal basis, then the equation*

$$Tv = 0$$

has always the unique orthogonal solution $0 \in V$.

3 The vector space of functions $\mathbf{F}_q^n \rightarrow \mathbf{F}_q$

In the next subsection we review the well known result that any function $F : K^n \rightarrow K$, where K is a finite field and $n \in \mathbb{N}$, is a polynomial function. Furthermore, we introduce the family of fundamental monomial functions.

3.1 The ring of polynomial functions in n variables over \mathbf{F}_q and the vector space of functions $\mathbf{F}_q^n \rightarrow \mathbf{F}_q$

Definition 12 *We will denote a finite field with \mathbf{F}_q , where q stands for the number of elements of the field (q is a power of the prime characteristic of the field).*

Definition 13 (Notational definition) *We call a commutative Ring $(R, +, \cdot)$ with multiplicative identity $1 \neq 0$ and the binary operations \cdot and $+$ just Ring R .*

The following three results are well known:

Theorem 14 (and Definition) *Let R be a ring and $n \in \mathbb{N}$ a natural number. The set*

$$PF_n(R) := \{g \mid g : R^n \rightarrow R \text{ is polynomial}\}$$

together with the common operations $+$ and \cdot of addition and multiplication of mappings is a ring. This ring is called ring of all polynomial functions over R in n R -valued variables.

Theorem 15 (and Definition) *Let K be an arbitrary field and $n \in \mathbb{N}$ a natural number. The set of all functions*

$$f : K^n \rightarrow K$$

together with the common operations of addition of mappings and scalar multiplication is a vector space over K . We denote this vector space with $F_n(K)$.

Theorem 16 *Let \mathbf{F}_q be a finite field. Then for the sets $F_n(\mathbf{F}_q)$ and $PF_n(\mathbf{F}_q)$ it holds*

$$F_n(\mathbf{F}_q) = PF_n(\mathbf{F}_q)$$

Proof. This result is proved in Chapter 7, Section 5 of (Lidl & Niederreiter, 1997). ■

Definition 17 *Let $n, q \in \mathbb{N}$ be natural numbers. Further let $>$ be a total ordering on $(\mathbb{N}_0)^n$. The according to $>$ decreasingly ordered set*

$$M_q^n := \{\alpha \in (\mathbb{N}_0)^n \mid \alpha_j < q \ \forall j \in \{1, \dots, n\}\}$$

of all n -tuples with entries smaller than q is denoted by $M_q^n \subset (\mathbb{N}_0)^n$.

Remark 18 *In order to avoid a too complicated notation, we skip the appearance of the order relation $>$ in the symbol for this set. It is easy to prove, that M_q^n contains exactly q^n n -tuples. We will index the n -tuples in M_q^n starting with the biggest and ending with the smallest:*

$$\alpha_1 > \alpha_2 > \dots > \alpha_{q^n}$$

Definition 19 *For any fixed natural numbers $n, q \in \mathbb{N}$ and for each multi index $\alpha \in M_q^n$ consider the monomial function*

$$\begin{aligned} g_{nq\alpha} & : K^n \rightarrow K \\ \vec{x} & \mapsto g_{nq\alpha}(\vec{x}) := \vec{x}^\alpha \end{aligned}$$

All these monomial functions $g_{nq\alpha}$, $\alpha \in M_q^n$ are called fundamental monomial functions.

The following result is elementary. Its easy induction proof is left to the reader:

Theorem 20 *A basis for the vector space $F_n(\mathbf{F}_q)$ is given by the fundamental monomial functions*

$$(g_{nq\alpha})_{\alpha \in M_q^n}$$

Remark 21 *The basis elements in the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$ are ordered according to the order relation $>$ used to order the n -tuples in the set M_q^n . That means (see Remark 18)*

$$(g_{nq\alpha})_{\alpha \in M_q^n} = (g_{nq\alpha_i})_{i \in \{1, \dots, q^n\}}$$

3.2 Solving the polynomial interpolation problem in $PF_n(\mathbf{F}_q)$

In this subsection we define the *evaluation epimorphism* of a tuple $(\vec{x}_1, \dots, \vec{x}_m) \in (\mathbf{F}_q^n)^m$ of points in the space \mathbf{F}_q^n . The evaluation epimorphism allows for a linear algebraic formulation of the multivariate polynomial interpolation problem.

Theorem 22 (and Definition) *Let \mathbf{F}_q be a finite field and $n, m \in \mathbb{N}$ natural numbers with $m \leq q^n$. Further let*

$$\vec{X} := (\vec{x}_1, \dots, \vec{x}_m) \in (\mathbf{F}_q^n)^m$$

*be a tuple of m **different** n -tuples with entries in the field \mathbf{F}_q . Then the mapping*

$$\begin{aligned} \Phi_{\vec{X}} &: F_n(\mathbf{F}_q) \rightarrow \mathbf{F}_q^m \\ f &\mapsto \Phi_{\vec{X}}(f) := (f(\vec{x}_1), \dots, f(\vec{x}_m))^t \end{aligned}$$

is a surjective linear operator. $\Phi_{\vec{X}}$ is called the evaluation epimorphism of the tuple \vec{X} .

Proof. The proof of the linearity is left to the reader. Now let $\vec{b} \in \mathbf{F}_q^m$ be an arbitrary vector. Since $m \leq q^n$ we can construct a function

$$g \in F_n(\mathbf{F}_q)$$

with the property

$$g(\vec{x}_i) = b_i \quad \forall i \in \{1, \dots, m\}$$

and that means exactly

$$\Phi_{\vec{X}}(g) = \vec{b} \quad \blacksquare$$

Remark 23 (and Corollary) *Since a basis of $F_n(\mathbf{F}_q)$ is given by the fundamental monomial functions $(g_{nq\alpha})_{\alpha \in M_q^n}$, the matrix*

$$A := (\Phi_{\vec{X}}(g_{nq\alpha}))_{\alpha \in M_q^n} \in M(m \times q^n; \mathbf{F}_q)$$

representing the evaluation epimorphism $\Phi_{\vec{X}}$ of the tuple \vec{X} with respect to the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$ of $F_n(\mathbf{F}_q)$ and the canonical basis of \mathbf{F}_q^m has always the full rank $m = \min(m, q^n)$. That also means, that the dimension of the $\ker(\Phi_{\vec{X}})$ is

$$\dim(\ker(\Phi_{\vec{X}})) = \dim(F_n(\mathbf{F}_q)) - m = q^n - m$$

Corollary 24 *Let \mathbf{F}_q be a finite field and $n, m \in \mathbb{N}$ natural numbers with $m \leq q^n$. Further let*

$$\vec{X} := (\vec{x}_1, \dots, \vec{x}_m) \in (\mathbf{F}_q^n)^m$$

be a tuple of m different n -tuples with entries in the field \mathbf{F}_q and $\vec{b} \in \mathbf{F}_q^m$ a vector. Then the interpolation problem of finding a polynomial function $f \in PF_n(\mathbf{F}_q)$ with the property

$$f(\vec{x}_i) = b_i \quad \forall i \in \{1, \dots, m\}$$

can be solved by solving the system of linear equations

$$A\vec{y} = \vec{b} \tag{3}$$

where

$$A := (\Phi_{\vec{X}}(g_{nq\alpha}))_{\alpha \in M_q^n}$$

is the matrix representing the evaluation epimorphism $\Phi_{\vec{X}}$ of the tuple \vec{X} with respect to the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$ of $F_n(\mathbf{F}_q)$ and the canonical basis of \mathbf{F}_q^m . The entries of a solution vector of the equations (3) are the coefficients of the solution with respect to the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$.

Proof. Since $F_n(\mathbf{F}_q) = PF_n(\mathbf{F}_q)$, a solution of the interpolation problem can be found by solving the equation

$$\Phi_{\vec{X}}(g) = \vec{b} \quad (4)$$

for g , where $\Phi_{\vec{X}}$ is the surjective linear operator

$$\begin{aligned} \Phi_{\vec{X}} &: F_n(\mathbf{F}_q) \rightarrow \mathbf{F}_q^m \\ f &\mapsto \Phi_{\vec{X}}(f) := (f(\vec{x}_1), \dots, f(\vec{x}_m))^t \end{aligned}$$

of the above theorem. After fixing the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$ of $F_n(\mathbf{F}_q)$ and the canonical basis of \mathbf{F}_q^m , equation (4) implies the following system of linear equations for the coefficients of the solutions with respect to the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$

$$A\vec{y} = \vec{b}$$

where

$$A := (\Phi_{\vec{X}}(g_{nq\alpha}))_{\alpha \in M_q^n}$$

is the matrix representing the map $\Phi_{\vec{X}}$ with respect to the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$ of $F_n(\mathbf{F}_q)$ and the canonical basis of \mathbf{F}_q^m . According to Remark 23, the matrix A has full rank and therefore a solution of $A\vec{y} = \vec{b}$ always exists. ■

4 Construction of special purpose symmetric bilinear forms

Let \mathbf{F}_q be a finite field and $n, m \in \mathbb{N}$ natural numbers with $m < q^n$. Further let

$$\vec{X} := (\vec{x}_1, \dots, \vec{x}_m) \in (\mathbf{F}_q^n)^m$$

be a tuple of m different n -tuples with entries in the field \mathbf{F}_q and $d := \dim(F_n(\mathbf{F}_q))$. Now consider the evaluation epimorphism $\Phi_{\vec{X}}$ of the tuple \vec{X} . By Remark 23 and due to the fact $m < q^n$, the nullity of $\Phi_{\vec{X}}$ is given by

$$s := \dim(\ker(\Phi_{\vec{X}})) = \dim(F_n(\mathbf{F}_q)) - m = q^n - m > 0$$

Now let (u_1, \dots, u_s) be a basis of $\ker(\Phi_{\vec{X}}) \subseteq F_n(\mathbf{F}_q)$. By the basis extension theorem, we can extend the basis (u_1, \dots, u_s) to a basis

$$(u_1, \dots, u_s, u_{s+1}, \dots, u_d)$$

of the whole space $F_n(\mathbf{F}_q)$. As in example 6, we can construct a symmetric bilinear form on $F_n(\mathbf{F}_q)$ by setting

$$\langle u_i, u_j \rangle := \delta_{ij} \quad \forall i, j \in \{1, \dots, d\}$$

Here the basis (u_1, \dots, u_d) is orthonormal and the vectors (u_{s+1}, \dots, u_d) are a basis of the orthogonal complement $\ker(\Phi_{\vec{X}})^\perp$ of $\ker(\Phi_{\vec{X}})$.

In general, the way we extend the basis (u_1, \dots, u_s) of $\ker(\Phi_{\vec{X}})$ to a basis

$$(u_1, \dots, u_s, u_{s+1}, \dots, u_d)$$

of the whole space $F_n(\mathbf{F}_q)$ determines crucially the symmetric bilinear form we get by setting $\langle u_i, u_j \rangle := \delta_{ij} \forall i, j \in \{1, \dots, d\}$. Consequently, the orthogonal solution of $\Phi_{\vec{X}}(g) = \vec{b}$ may vary according to the chosen extension $u_{s+1}, \dots, u_d \in F_n(\mathbf{F}_q)$. One systematic way to get a basis of the whole space $F_n(\mathbf{F}_q)$ starting with a basis (u_1, \dots, u_s) of $\ker(\Phi_{\vec{X}})$ is the following: let

$$(\vec{y}_1, \dots, \vec{y}_s)^t \quad (5)$$

be the matrix whose rows are the coordinate vectors $\vec{y}_1, \dots, \vec{y}_s \in K^d$ of (u_1, \dots, u_s) with respect to the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$ of $F_n(\mathbf{F}_q)$. Now we perform Gauss-Jordan elimination on the matrix (5), obtaining the matrix R . Now consider the set $B := \{\vec{e}_1, \dots, \vec{e}_d\}$ of canonical unit vectors of the space \mathbf{F}_q^d . For every pivot element r_{ij} used during the Gauss-Jordan elimination performed on (5), eliminate the canonical unit vector \vec{e}_j from the set B . This yields the set \tilde{B} . The coordinate vectors for a basis for the whole space $F_n(\mathbf{F}_q)$ are now given by the the rows of R and the vectors in the set \tilde{B} . We call this way of construction of the orthonormal basis for the space $F_n(\mathbf{F}_q)$ the *standard orthonormalization*. We illustrate the algorithm using an example:

Example 25 Suppose $q = 3$, $\mathbf{F}_3 = \mathbb{Z}_3$, $m = 4$, $d = 3^2 = 9$, $s = 5$ and that after performing Gauss-Jordan elimination on (5) we get the following matrix

$$R := \begin{pmatrix} 1 & 0 & z_{1,3} & 0 & 0 & z_{1,6} & 0 & z_{1,8} & z_{1,9} \\ 0 & 1 & z_{2,3} & 0 & 0 & z_{2,6} & 0 & z_{2,8} & z_{2,9} \\ 0 & 0 & 0 & 1 & 0 & z_{3,6} & 0 & z_{3,8} & z_{3,9} \\ 0 & 0 & 0 & 0 & 1 & z_{4,6} & 0 & z_{4,8} & z_{4,9} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & z_{5,8} & z_{5,9} \end{pmatrix} \quad (6)$$

(The $z_{i,j} \in \mathbf{F}_q$ stand for unspecified field elements). Then for the extension of the basis we choose the following canonical basis vectors

$$\vec{e}_3, \vec{e}_6, \vec{e}_8, \vec{e}_9 \in \mathbb{Z}_3^9$$

Now we substitute coordinate vectors $(\vec{y}_1, \dots, \vec{y}_5)$ of the basis (u_1, \dots, u_5) by the rows in the reduced matrix 6 (this step is not strictly necessary, but it will be needed to prove the theorems below) and get the following coordinate vectors for a basis for the whole space $F_2(\mathbb{Z}_3)$

$$(\vec{y}_1, \dots, \vec{y}_s, \vec{y}_{s+1}, \dots, \vec{y}_d) := (R^t, \vec{e}_3, \vec{e}_6, \vec{e}_8, \vec{e}_9)$$

In this specific example we use the standard lexicographic ordering on $(\mathbb{N}_0)^2$ and so we have

$$M_3^2 = \{(2, 2), (2, 1), (2, 0), (1, 2), (1, 1), (1, 0), (0, 2), (0, 1), (0, 0)\}$$

and

$$(g_{23\alpha}(\vec{x}))_{\alpha \in M_3^2} = (x_2^2 x_1^2, x_2^2 x_1, x_2^2, x_2 x_1^2, x_2 x_1, x_2, x_1^2, x_1, 1)$$

Thus the orthonormal basis $(\vec{u}_1, \dots, \vec{u}_s, u_{s+1}, \dots, u_d)$ of $F_2(\mathbb{Z}_3)$ evaluated at the point $\vec{x} \in \mathbb{Z}_3^2$ would be

$$\begin{pmatrix} x_2^2 x_1^2 + z_{1,3} x_2^2 + z_{1,6} x_2 + z_{1,8} x_1 + z_{1,9} \\ x_2 x_1^2 + z_{2,3} x_2^2 + z_{2,6} x_2 + z_{2,8} x_1 + z_{2,9} \\ x_2 x_1^2 + z_{3,6} x_2 + z_{3,8} x_1 + z_{3,9} \\ x_2 x_1 + z_{4,6} x_2 + z_{4,8} x_1 + z_{4,9} \\ x_1^2 + z_{5,8} x_1 + z_{5,9} \\ x_2^2 \\ x_2 \\ x_1 \\ 1 \end{pmatrix}^t$$

and the orthogonal solution of $\Phi_{\vec{X}}(g) = \vec{b}$ is a vector in $\text{Span}(x_2^2, x_2, x_1, 1)$.

In the next section, we will establish the exact relationship between the orthogonal solution of $\Phi_{\vec{X}}(g) = \vec{b}$ (using the symmetric bilinear form defined above) and the normal form with respect to the vanishing ideal $I(X)$. This relationship can be established if the order relation $>$ used to order the n -tuples in the set M_q^n is a *monomial ordering*. If, more generally, total orderings on $(\mathbb{N}_0)^n$ are used to order the set M_q^n , the set of possible orthogonal solutions of $\Phi_{\vec{X}}(g) = \vec{b}$ can be seen as a wider class of normal forms (with respect to vanishing ideals) in which the "classical" normal forms (attached to monomial orderings) appear as special cases.

5 Orthogonal solutions of $\Phi_{\vec{X}}(g) = \vec{b}$ and the normal form with respect to the vanishing ideal $I(X)$

In this section we will show the main result of this article: Given a set of points $X \subset K^n$, an arbitrary polynomial $f \in K[\tau_1, \dots, \tau_n]$ and a monomial order $>$, the normal form of f with respect to the vanishing ideal $I(X) \subseteq K[\tau_1, \dots, \tau_n]$ can be calculated as the orthogonal solution of

$$\Phi_{\vec{X}}(g) = \vec{b}$$

where \vec{b} is given by

$$b_i := \tilde{f}(\vec{x}_i), \quad i = 1, \dots, m$$

The yet undefined notation \tilde{f} suggests that a mapping between the ring $K[\tau_1, \dots, \tau_n]$ of polynomials and the vector space of functions $F_n(\mathbf{F}_q)$ is needed. That mapping will be defined and characterized in the first lemma and theorem of this section. After introducing some notation we arrive at an important preliminary result in Theorem 30, which states how a (particular) basis of $\ker(\Phi_{\vec{X}})$ can be extended to a Gröbner basis of $I(X)$. With that result our goal can be easily reached. Please note that through this section a more technical result stated and proved in the appendix is used.

Lemma 26 (and Definition) *Let K be a field, $n, q \in \mathbb{N}$ natural numbers and $K[\tau_1, \dots, \tau_n]$ the polynomial ring in n indeterminates over K . Then the set of all polynomials of the form*

$$\sum_{\alpha \in M_q^n} a_\alpha \tau_1^{\alpha_1} \dots \tau_n^{\alpha_n} \in K[\tau_1, \dots, \tau_n]$$

with coefficients $a_\alpha \in K$ is a vector space over K . We denote this set with $P_q^n(K) \subset K[\tau_1, \dots, \tau_n]$.

Proof. The easy proof is left to the reader. ■

Theorem 27 *Let \mathbf{F}_q be a finite field and $n \in \mathbb{N}$ a natural number. Then the vector spaces $P_q^n(\mathbf{F}_q)$ and $F_n(\mathbf{F}_q)$ are isomorphic.*

Proof. After defining the linear mapping

$$\begin{aligned} \varphi &: P_q^n(\mathbf{F}_q) \rightarrow F_n(\mathbf{F}_q) \\ g &= \sum_{\alpha \in M_q^n} a_\alpha \tau_1^{\alpha_1} \dots \tau_n^{\alpha_n} \mapsto \varphi(g)(\vec{x}) := \sum_{\alpha \in M_q^n} a_\alpha \vec{x}^\alpha \end{aligned}$$

the claim follows easily. ■

Remark 28 (and Definition) The mapping φ is defined on the set $P_q^n(K) \subset K[\tau_1, \dots, \tau_n]$, but of course it can naturally be extended to $K[\tau_1, \dots, \tau_n]$ as

$$\begin{aligned} \varphi &: K[\tau_1, \dots, \tau_n] \rightarrow F_n(\mathbf{F}_q) \\ g &= \sum_{\alpha \in \Gamma} a_\alpha \tau_1^{\alpha_1} \dots \tau_n^{\alpha_n} \mapsto \varphi(g)(\vec{x}) := \sum_{\alpha \in \Gamma} a_\alpha \vec{x}^\alpha \end{aligned}$$

where Γ is a finite set of multi indexes. We denote the image under $\varphi : K[\tau_1, \dots, \tau_n] \rightarrow F_n(\mathbf{F}_q)$ of a polynomial $g \in K[\tau_1, \dots, \tau_n]$ with

$$\tilde{g} := \varphi(g) \in F_n(\mathbf{F}_q)$$

Definition 29 Let $d \in \mathbb{N}$ be a natural number, V a d -dimensional vector space over a field K and F a basis of V . Furthermore, let $U \subset V$ be an arbitrary proper subspace of V . Now let $s := \dim(U) \in \mathbb{N}$. A basis (u_1, \dots, u_s) of U is called a cleaned kernel basis with respect to the basis F if the matrix $(\vec{y}_1, \dots, \vec{y}_s)^t$ whose rows are the coordinate vectors $\vec{y}_1, \dots, \vec{y}_s \in K^d$ of (u_1, \dots, u_s) with respect to the basis F is in reduced row echelon form.

For a tuple $\vec{x} = (x_1, \dots, x_n)$ we write $x := \{x_1, \dots, x_n\}$ for the set containing all the entries in the tuple \vec{x} .

Theorem 30 Let \mathbf{F}_q be a finite field, $n, m \in \mathbb{N}$ natural numbers with $m < q^n$ and $>$ a fixed monomial order. Further let

$$\vec{X} := (\vec{x}_1, \dots, \vec{x}_m) \in (\mathbf{F}_q^n)^m$$

be a tuple of m different n -tuples with entries in the field \mathbf{F}_q and $s := \dim(\ker(\Phi_{\vec{X}}))$. In addition, let (u_1, \dots, u_s) be a cleaned kernel basis of $\ker(\Phi_{\vec{X}}) \subseteq F_n(\mathbf{F}_q)$ with respect to the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$. Then the family of polynomials

$$(\tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n, \varphi^{-1}(u_1), \dots, \varphi^{-1}(u_s))$$

is a Gröbner basis of the vanishing ideal $I(X) \subseteq \mathbf{F}_q[\tau_1, \dots, \tau_n]$ with respect to the monomial order $>$.

Proof. The idea of the proof is to show that

$$U := (\tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n, \varphi^{-1}(u_1), \dots, \varphi^{-1}(u_s))$$

generates the ideal $I(X)$ and that for any polynomial $g \in I(X)$ the remainder on division of g by U is zero. According to a well known fact about Gröbner bases (see proposition 5.38 of (Becker & Weispfenning, 1993)) this is equivalent to U being a Gröbner basis for $I(X)$. For this proof, remember that the fundamental monomial functions $(g_{nq\alpha})_{\alpha \in M_q^n}$ are ordered decreasingly with respect to the order $>$.

Now let $g \in I(X) \subseteq \mathbf{F}_q[\tau_1, \dots, \tau_n]$ be an arbitrary polynomial in the vanishing ideal of X . Since

$$(\tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n)$$

is a universal Gröbner basis for $I(\mathbf{F}_q^n)$ (see Theorem 36 in the appendix), there is a unique $r \in \mathbf{F}_q[\tau_1, \dots, \tau_n]$ with the properties

1. No term of r is divisible by any of $LT(\tau_1^q - \tau_1) = \tau_1^q, LT(\tau_2^q - \tau_2) = \tau_2^q, \dots, LT(\tau_n^q - \tau_n) = \tau_n^q$. That means in particular $r \in P_q^n(\mathbf{F}_q)$.

2. There is a $q \in I(\mathbf{F}_q^n)$ such that $g = q + r$

This means that when we start to divide g by the (ordered) family U we get the intermediate result

$$g = q + r$$

where the remainder $r \in P_q^n(\mathbf{F}_q)$ and $q \in \langle \tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n \rangle = I(\mathbf{F}_q^n)$. If $r = 0$, then we are done and the remainder \bar{g}^U on division of g by U is zero. If $r \neq 0$, then we know from

$$r = g - q$$

that $r \in I(X)$ ($q \in I(\mathbf{F}_q^n) \subseteq I(X)$) and this is equivalent to

$$\tilde{r}(\vec{x}) = \varphi(r)(\vec{x}) = 0 \quad \forall \vec{x} \in \mathbf{F}_q^n \Leftrightarrow \tilde{r} \in \ker(\Phi_{\vec{X}})$$

Since (u_1, \dots, u_s) is a basis for $\ker(\Phi_{\vec{X}})$, there are unique $\lambda_i \in \mathbf{F}_q$, $i = 1, \dots, s$ with

$$\tilde{r} = \sum_{i=1}^s \lambda_i u_i$$

Applying the vector space isomorphism $\varphi^{-1} : F_n(\mathbf{F}_q) \rightarrow P_q^n(\mathbf{F}_q)$ to this equation yields

$$r = \sum_{i=1}^s \lambda_i \varphi^{-1}(u_i)$$

From the requirement on (u_1, \dots, u_s) to be a cleaned kernel basis of $\ker(\Phi_{\vec{X}})$ now follows for each $j \in \{1, \dots, s\}$, that the leading term

$$LT(\varphi^{-1}(u_j))$$

doesn't appear in the polynomials $\varphi^{-1}(u_i)$, $i \in \{1, \dots, s\} \setminus \{j\}$. Consequently, in the expression

$$\sum_{i=1}^s \lambda_i \varphi^{-1}(u_i)$$

no cancellation of the leading terms $LT(\varphi^{-1}(u_i))$, $i = 1, \dots, s$ can occur. Therefore, the division of $r = \sum_{i=1}^s \lambda_i \varphi^{-1}(u_i)$ by $(\varphi^{-1}(u_1), \dots, \varphi^{-1}(u_s))$ must yield

$$r = \sum_{i=1}^s \lambda_i \varphi^{-1}(u_i) + 0$$

and the remainder \bar{g}^U on division of g by U is zero. As a consequence,

$$g \in \langle \tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n, \varphi^{-1}(u_1), \dots, \varphi^{-1}(u_s) \rangle$$

and since $g \in I(X)$ was arbitrary

$$I(X) \subseteq \langle \tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n, \varphi^{-1}(u_1), \dots, \varphi^{-1}(u_s) \rangle$$

The inclusion

$$\langle \tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n, \varphi^{-1}(u_1), \dots, \varphi^{-1}(u_s) \rangle \subseteq I(X)$$

is given by the fact $u_1, \dots, u_s \in \ker(\Phi_{\vec{X}})$ and Theorem 36. Summarizing we can say

$$\langle \tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n, \varphi^{-1}(u_1), \dots, \varphi^{-1}(u_s) \rangle = I(X)$$

and for every $g \in I(X)$ the remainder \bar{g}^U on division of g by U is zero. Now proposition 5.38 of (Becker & Weispfenning, 1993) (see also the remarks after corollary 2, chapter 2, § 6 of (Cox *et al.*, 1997)) proves the claim. ■

Theorem 31 Let \mathbf{F}_q be a finite field, $n, m \in \mathbb{N}$ natural numbers with $m < q^n$ and $>$ a fixed monomial order. Further let

$$\vec{X} := (\vec{x}_1, \dots, \vec{x}_m) \in (\mathbf{F}_q^n)^m$$

be a tuple of m different n -tuples with entries in the field \mathbf{F}_q , $\vec{b} \in \mathbf{F}_q^m$ a vector, $d := \dim(F_n(\mathbf{F}_q))$ and $s := \dim(\ker(\Phi_{\vec{X}}))$. In addition, let (u_1, \dots, u_s) be a cleaned kernel basis of $\ker(\Phi_{\vec{X}}) \subseteq F_n(\mathbf{F}_q)$ with respect to the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$, $(u_1, \dots, u_s, u_{s+1}, \dots, u_d)$ an orthonormal basis of $F_n(\mathbf{F}_q)$ constructed using the standard orthonormalization and $f \in \mathbf{F}_q[\tau_1, \dots, \tau_n]$ a polynomial satisfying the interpolation conditions

$$\tilde{f}(\vec{x}_j) = b_j \quad \forall j \in \{1, \dots, m\}$$

Furthermore, let $U \subseteq I(X)$ be an arbitrary Gröbner basis of the vanishing ideal $I(X)$ with respect to the monomial order $>$ and v^* the orthogonal solution of $\Phi_{\vec{X}}(g) = \vec{b}$. Then

$$\varphi^{-1}(v^*) = \bar{f}^U$$

Proof. If $\varphi^{-1}(v^*) = 0$ then $v^* = 0$ and

$$\vec{b} = \Phi_{\vec{X}}(v^*) = \Phi_{\vec{X}}(0) = \vec{0}$$

In this case we also have

$$\bar{f}^U = 0$$

and therefore

$$\varphi^{-1}(v^*) = \bar{f}^U$$

Assume $\varphi^{-1}(v^*) \neq 0$. Since the remainder on division by a Gröbner basis is independent of which Gröbner basis we use (for a fixed monomial order), the idea of the proof is to show that $\varphi^{-1}(v^*)$ is the unique remainder on division by the Gröbner basis

$$(\tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n, \varphi^{-1}(u_1), \dots, \varphi^{-1}(u_s))$$

(see Theorem 30). Now, since $\varphi^{-1}(v^*) \in P_q^n(\mathbf{F}_q)$, no term of $\varphi^{-1}(v^*)$ is divisible by any of the

$$LT(\tau_1^q - \tau_1) = \tau_1^q, LT(\tau_2^q - \tau_2) = \tau_2^q, \dots, LT(\tau_n^q - \tau_n) = \tau_n^q$$

If terms of $\varphi^{-1}(v^*)$ would be divisible by

$$LT(\varphi^{-1}(u_1)), \dots, LT(\varphi^{-1}(u_s))$$

then after division by the family

$$(\tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n, \varphi^{-1}(u_1), \dots, \varphi^{-1}(u_s))$$

we would have

$$\varphi^{-1}(v^*) = \sum_{i=1}^s h_i \varphi^{-1}(u_i) + r \tag{7}$$

where $h_i, r \in \mathbf{F}_q[\tau_1, \dots, \tau_n]$, $i = 1, \dots, s$ and either $r = 0$ or no term of r is divisible by the

$$LT(\tau_1^q - \tau_1), \dots, LT(\tau_n^q - \tau_n), LT(\varphi^{-1}(u_1)), \dots, LT(\varphi^{-1}(u_s))$$

If $r = 0$, then

$$\varphi^{-1}(v^*) = \sum_{i=1}^s h_i \varphi^{-1}(u_i)$$

and the polynomial $\varphi^{-1}(v^*)$ vanishes on the set X , that is

$$\varphi(\varphi^{-1}(v^*))(\vec{x}) = v^*(\vec{x}) = 0 \quad \forall \vec{x} \in X$$

Consequently

$$\vec{b} = \Phi_{\vec{X}}(v^*) = \vec{0}$$

and due to the uniqueness of the orthogonal solution

$$v^* = 0$$

But this is a contradiction to our assumption $\varphi^{-1}(v^*) \neq 0$.

Now if $r \neq 0$, since no term of r is divisible by $LT(\tau_1^q - \tau_1), \dots, LT(\tau_n^q - \tau_n)$, then in particular $r \in P_q^n(\mathbf{F}_q)$. Due to the fact, that $(u_1, \dots, u_s, u_{s+1}, \dots, u_d)$ is a basis for $F_n(\mathbf{F}_q)$, we can write

$$\tilde{r} = \varphi(r) = \sum_{j=1}^d \lambda_j u_j$$

with unique $\lambda_j \in \mathbf{F}_q$, $j = 1, \dots, d$. Applying the vector space isomorphism $\varphi^{-1} : F_n(\mathbf{F}_q) \rightarrow P_q^n(\mathbf{F}_q)$ to this equation yields

$$r = \sum_{j=1}^d \lambda_j \varphi^{-1}(u_j)$$

From the requirement on (u_1, \dots, u_s) to be a cleaned kernel basis of $\ker(\Phi_{\vec{X}})$ with respect to the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$ and since the basis extension $(u_1, \dots, u_s, u_{s+1}, \dots, u_d)$ has been constructed using the standard orthonormalization, in the expression

$$\sum_{j=1}^d \lambda_j \varphi^{-1}(u_j)$$

no cancellation of the leading terms $LT(\varphi^{-1}(u_k))$, $k = 1, \dots, s$ can occur. But r is not divisible by $LT(\varphi^{-1}(u_1)), \dots, LT(\varphi^{-1}(u_s))$ and that forces

$$\lambda_k = 0, \quad \forall k \in \{1, \dots, s\}$$

In other words

$$r = \sum_{j=s+1}^d \lambda_j \varphi^{-1}(u_j) \Leftrightarrow \tilde{r} = \varphi(r) = \sum_{j=s+1}^d \lambda_j u_j$$

which is equivalent to

$$\tilde{r} \in \ker(\Phi_{\vec{X}})^\perp \tag{8}$$

From the equation (7) we know that

$$r = \varphi^{-1}(v^*) - \sum_{i=1}^s h_i \varphi^{-1}(u_i)$$

and that means

$$\tilde{r}(\vec{x}) = v^*(\vec{x}) \quad \forall \vec{x} \in X$$

In other words

$$\Phi_{\vec{X}}(\tilde{r}) = \vec{b}$$

This together with (8) says that \tilde{r} is an orthogonal solution of $\Phi_{\vec{X}}(g) = \vec{b}$. From the uniqueness now follows

$$v^* = \tilde{r} \Leftrightarrow \varphi^{-1}(v^*) = r$$

Consequently, no term of the polynomial $\varphi^{-1}(v^*)$ is divisible by any of the leading terms of the elements of the Gröbner basis (see Theorem 30)

$$G := (\tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n, \varphi^{-1}(u_1), \dots, \varphi^{-1}(u_s))$$

for the vanishing ideal $I(X)$. Now we define the polynomial

$$h := f - \varphi^{-1}(v^*)$$

Since v^* is a solution of $\Phi_{\vec{X}}(g) = \vec{b}$ and f satisfies the interpolation conditions

$$\tilde{f}(\vec{x}_j) = b_j \quad \forall j \in \{1, \dots, m\}$$

we have

$$\tilde{h}(\vec{x}) = \tilde{f}(\vec{x}) - v^*(\vec{x}) = 0 \quad \forall \vec{x} \in X \Leftrightarrow h \in I(X)$$

So we have a polynomial $h \in I(X)$ such that

$$f = h + \varphi^{-1}(v^*)$$

By proposition 1, chapter 2, §6 in (Cox *et al.*, 1997), $\varphi^{-1}(v^*)$ is the unique remainder on division by the Gröbner basis G . It is a well known fact, that the remainder on division by a Gröbner basis is independent of which Gröbner basis we use, as long as we use one fixed particular monomial order. Therefore

$$\overline{f}^U = \overline{f}^G = \varphi^{-1}(v^*) \quad \blacksquare$$

Remark 32 (and main theorem) Let \mathbf{F}_q be a finite field, $n, m \in \mathbb{N}$ natural numbers with $m < q^n$ and $>$ a fixed monomial order. Further let

$$\vec{X} := (\vec{x}_1, \dots, \vec{x}_m) \in (\mathbf{F}_q^n)^m$$

be a tuple of m different n -tuples with entries in the field \mathbf{F}_q , $U \subseteq I(X)$ an arbitrary Gröbner basis of the vanishing ideal $I(X)$ and $f \in \mathbf{F}_q[\tau_1, \dots, \tau_n]$ an arbitrary polynomial. Then

$$\overline{f}^U = \varphi^{-1}(v^*)$$

where v^* is the orthogonal solution of $\Phi_{\vec{X}}(g) = \vec{b}$ and \vec{b} is given by

$$b_i := \tilde{f}(\vec{x}_i), \quad i = 1, \dots, m$$

Remark 33 *Let*

$$A := (\Phi_{\vec{X}}(g_{nq\alpha}))_{\alpha \in M_q^n} \in M(m \times q^n; \mathbf{F}_q)$$

be the matrix representing the evaluation epimorphism $\Phi_{\vec{X}}$ of the tuple \vec{X} with respect to the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$ of $F_n(\mathbf{F}_q)$ and the canonical basis of \mathbf{F}_q^m and S the matrix

$$S_{ij} := \langle g_{nq\alpha_i}, g_{nq\alpha_j} \rangle, \quad i, j \in \{1, \dots, q^n\}$$

representing the symmetric bilinear form with respect to the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$. Further let $\vec{y}_1, \dots, \vec{y}_s \in \mathbf{F}_q^d$ be the coordinate vectors of (u_1, \dots, u_s) with respect to the basis $(g_{nq\alpha})_{\alpha \in M_q^n}$. Then the above result states that the normal form \vec{f}^U of f with respect to the Gröbner basis $U \subseteq I(X)$ can be calculated by solving the following system of inhomogeneous linear equations

$$\begin{aligned} A\vec{z} &= \vec{b} \\ \vec{y}_i^t S\vec{z} &= 0, \quad i = 1, \dots, s \end{aligned}$$

6 Acknowledgements

We would like to thank Dr. Gretchen Matthews, Dr. Michael Shapiro and Dr. Michael Stillman for very helpful comments and contributions for the content of this paper.

7 Appendix

Lemma 34 *Let K be a field, $n \in \mathbb{N}$ a natural number, $K[\tau_1, \dots, \tau_n]$ the polynomial ring in n indeterminates over K and $>$ an arbitrary monomial order. Then for each natural number $m \in \mathbb{N}$ and each $i \in \{1, \dots, n\}$ it holds*

$$\tau_i^m > \tau_i^{m-1} > \dots > \tau_i > \tau_i^0 \quad (9)$$

Proof. The claim follows from the well-ordering, the translation invariance and transitivity of $>$. ■

Theorem 35 *Let \mathbf{F}_q be a finite field and $n \in \mathbb{N}$ a natural number. Then the family of polynomials*

$$(\tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n)$$

is a basis for the vanishing ideal

$$I(\mathbf{F}_q^n) \subseteq \mathbf{F}_q[\tau_1, \dots, \tau_n]$$

Proof. The proof of this well-known result can be found after Lemma 3.1 of (Germundsson, 1991). ■

Theorem 36 *Let \mathbf{F}_q be a finite field and $n \in \mathbb{N}$ a natural number. Then the family of polynomials*

$$(\tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n)$$

is a universal Gröbner basis for the vanishing ideal

$$I(\mathbf{F}_q^n) \subseteq \mathbf{F}_q[\tau_1, \dots, \tau_n]$$

Proof. From the inequalities 9 it follows in particular for all possible monomial orders

$$LM(\tau_i^q - \tau_i) = \tau_i^q \forall i \in \{1, \dots, n\}$$

As a consequence, for the least common multiple (*LCM*) of $LM(\tau_j^q - \tau_j)$ and $LM(\tau_i^q - \tau_i)$, $i \neq j$ holds

$$LCM(LM(\tau_j^q - \tau_j), LM(\tau_i^q - \tau_i)) = LCM(\tau_j^q, \tau_i^q) = \tau_j^q \tau_i^q \forall i, j \in \{1, \dots, n\} \text{ with } i \neq j$$

and for the *S*-polynomial of $\tau_j^q - \tau_j$ and $\tau_i^q - \tau_i$, $i \neq j$ we have

$$S(\tau_j^q - \tau_j, \tau_i^q - \tau_i) = \tau_i^q(\tau_j^q - \tau_j) - \tau_j^q(\tau_i^q - \tau_i) = \tau_j^q \tau_i - \tau_i^q \tau_j \forall i, j \in \{1, \dots, n\} \text{ with } i \neq j$$

Now let's divide $S(\tau_j^q - \tau_j, \tau_i^q - \tau_i) = \tau_j^q \tau_i - \tau_i^q \tau_j$ by $(\tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n)$. Without loss of generality let

$$\tau_j^q \tau_i > \tau_i^q \tau_j$$

(which is equivalent to $LT(\tau_j^q \tau_i - \tau_i^q \tau_j) = \tau_j^q \tau_i$). Then, after the first division step, we get the remainder

$$-\tau_i^q \tau_j + \tau_i \tau_j$$

Now we know from the inequalities (9) after translation by τ_j

$$\tau_i^q \tau_j > \tau_i \tau_j \Rightarrow LT(-\tau_i^q \tau_j + \tau_i \tau_j) = -\tau_i^q \tau_j$$

so we can continue the division process and we get the remainder

$$-\tau_i^q \tau_j + \tau_i \tau_j - (-\tau_j)(\tau_i^q - \tau_i) = 0$$

By the theorem above

$$I(\mathbf{F}_q^n) = \langle \tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n \rangle$$

And so, according to Buchberger's *S*-pair criterion (see Theorem 6 of chapter 2, §6 in (Cox *et al.*, 1997)),

$$(\tau_1^q - \tau_1, \tau_2^q - \tau_2, \dots, \tau_n^q - \tau_n)$$

is a universal Gröbner Basis for $I(\mathbf{F}_q^n)$. ■

References

- Barbieri, F., & Facchinetti, G. 1973. Osservazioni sopra alcune definizioni di pseudo-prodotti interni. *Atti Sem. Mat. Fis. Univ. Modena*, **22**, 48–59 (1974).
- Becker, T., & Weispfenning, V. 1993. *Gröbner bases*. Graduate Texts in Mathematics, vol. 141. New York: Springer-Verlag. A computational approach to commutative algebra, In cooperation with Heinz Kredel.
- Buchberger, B. 1970. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Math.*, **4**, 374–383.
- Buchberger, B. 1976. A theoretical basis for the reduction of polynomials to canonical forms. *ACM SIGSAM Bull.*, **10**(3), 19–29.

-
- Cox, D., Little, J., & O'Shea, D. 1997. *Ideals, varieties, and algorithms, An introduction to computational algebraic geometry and commutative algebra*. Second edn. Undergraduate Texts in Mathematics. New York: Springer-Verlag.
- Degani Cattelani, F., & Fiocchi, C. 1974. Problema degli autovalori in spazi con prodotto pseudo-interno. *Atti Sem. Mat. Fis. Univ. Modena*, **23**(1), 55–69 (1975).
- Degani Cattelani, F., & Fiocchi, C. 1975. Spettro simmetrico e rango numerico di un operatore non lineare in spazi con prodotto pseudo-interno. *Atti Sem. Mat. Fis. Univ. Modena*, **24**(1), 88–105 (1976).
- Germundsson, R. 1991 (Sep). *Basic results on ideals and varieties in finite fields*. Tech. rept. LiTH-ISY-I-1259. Linkping University, Linkping, Sweden.
- Kasahara, S. 1980. Linear independency of linear space valued mappings and pseudo-inner-products. *Math. Japon.*, **25**(3), 321–325.
- Laubenbacher, R., & Stigler, B. 2004. A computational algebra approach to the reverse engineering of gene regulatory networks. *J. Theoret. Biol.*, **229**(4), 523–537.
- Lauer, M. 1976. Canonical representatives for residue classes of a polynomial ideal. *Pages 339–345 of: SYMSAC '76: Proceedings of the third ACM symposium on Symbolic and algebraic computation*. New York, NY, USA: ACM Press.
- Lidl, R., & Niederreiter, H. 1997. *Finite fields*. Second edn. Encyclopedia of Mathematics and its Applications, vol. 20. Cambridge: Cambridge University Press. With a foreword by P. M. Cohn.
- Lumer, G. 1961. Semi-inner-product spaces. *Trans. Amer. Math. Soc.*, **100**, 29–43.
- Mininni, M., & Muni, G. 1979. A degree theory with respect to a pseudo-inner product in a locally convex vector space. *Ricerche Mat.*, **28**(2), 365–374.
- Scharlau, W. 1969. *Quadratic forms*. Queen's papers in pure and applied mathematics, vol. 22. Kingston, Ontario: Queen's University.
- Vasanthan, W. B., & Johnson, T. 2003. New spectral theorem for vector spaces over finite fields Z_p . *Varāhmihir J. Math. Sci.*, **3**(2), 355–364.